#3

PATENT
P56339

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

YOUNG-IL KIM

Serial No.: *to be assigned* Examiner: *to be assigned*

Filed: 6 July 2001 Art Unit: *to be assigned*

For: MAC ADDRESS-BASED COMMUNICATION RESTRICTING METHOD

CLAIM OF PRIORITY
UNDER 35 U.S.C. §119

Assistant Commissioner
for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application, Korean Priority No. 2000/38560 (filed in Korea on 6 July 2000, and filed in the U.S. Patent and Trademark Office on 6 July 2001), is hereby requested and the right of priority provided in 35 U.S.C. §119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application.

Respectfully submitted,

Robert E. Bushnell
Reg. No.: 27,774
Attorney for the Applicant

Suite 300, 1522 "K" Street, N.W.
Washington, D.C. 20005-1202
(202) 408-9040

Folio: P56339
Date: 6 July 2001
I.D.: REB/sys

대 한 민 국 특 허 청
KOREAN INDUSTRIAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Industrial Property Office.

출 원 번 호 : 특허출원 2000년 제 38560 호
Application Number

출 원 년 월 일 : 2000년 07월 06일
Date of Application

출 원 인 : 삼성전자 주식회사
Applicant(s)

2001 년 02 월 07 일

특 허 청
COMMISSIONER

【서류명】 특허출원서
【권리구분】 특허
【수신처】 특허청장
【참조번호】 0001
【제출일자】 2000.07.06
【국제특허분류】 H04M
【발명의 명칭】 미디어 억세스 제어 어드레스에 의한 통신제한방법
【발명의 영문명칭】 SECURE COMMUNICATING METHOD BY MAC ADDRESS
【출원인】
【명칭】 삼성전자 주식회사
【출원인코드】 1-1998-104271-3
【대리인】
【성명】 이건주
【대리인코드】 9-1998-000339-8
【포괄위임등록번호】 1999-006038-0
【발명자】
【성명의 국문표기】 김영일
【성명의 영문표기】 KIM,Young Il
【주민등록번호】 630327-1804329
【우편번호】 442-371
【주소】 경기도 수원시 팔달구 매탄1동 164-10 우성 APT 101-609
【국적】 KR
【심사청구】 청구
【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인
이건주 (인)
【수수료】
【기본출원료】 12 면 29,000 원
【가산출원료】 0 면 0 원
【우선권주장료】 0 건 0 원
【심사청구료】 1 항 141,000 원
【합계】 170,000 원
【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 이더넷 스위치에서 미디어억세스 제어 어스레스(Media Access Control Address)를 이용하여 시스템상에 특정 호스트를 지정하고 통신이 허가되는 노드들을 지정하여 레이어2(Layer 2)상에서 접근 권한 여부를 제어하는 MAC어드레스에 의한 통신제한방법에 관한 것이다.

미디어 억세스 제어 어드레스에 의한 통신제한방법에 있어서, 이더넷 스위치를 통해 통신요구가 있을 시 패킷데이터를 수신하는 과정과, 상기 수신한 패킷데이터의 패킷 어드레스와 소스어드레스를 독출하여 각 어드레스의 엔트리 테이블 억세스 벡터가 일치하는지 검출하는 과정과, 상기 엔트리 테이블 억세스벡터가 일치하지 않을 시 접속을 차단하는 과정으로 이루어짐을 특징으로 한다.

【대표도】

도 1

【색인어】

이더넷 스위치, MAC

【명세서】

【발명의 명칭】

미디어 억세스 제어 어드레스에 의한 통신제한방법{SECURE COMMUNICATING METHOD BY MAC ADDRESS}

【도면의 간단한 설명】

도 1은 본 발명의 실시예에 따른 패킷 스위치 장치의 일예도

도 2는 본 발명의 실시예에 따른 미디어 억세스 제어어드레스에 의해 통신을 제한하기 위한 제어흐름도

도 3은 본 발명의 실시예에 따른 안티헤커 테이블 구성도

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<4> 본 발명은 이더넷 스위치의 통신제한 방법에 관한 것으로, 특히 이더넷 스위치에서 미디어억세스 제어 어스레스(Media Access Control Address)를 이용하여 시스템상에 특정 호스트를 지정하고 통신이 허가되는 노드들을 지정하여 레이어2(Layer 2)상에서 접근권한 여부를 제어하는 MAC어드레스에 의한 통신제한방법에 관한 것이다.

<5> 오늘날 점차적으로 데이터 네트워크(data network) 환경이 쉐어드 미디엄(shared medium)에서 스위치드 네트워크(switched network) 구조로 빠르게 변화하는 추세에 맞춰

기존의 허브(hub)를 고성능 저가격의 스위치로 대체할 이유가 상대적으로 증가하고 있다. 따라서, 새로운 시장의 요구와 추세에 맞는 언매니지드 저가격 이더넷 스위치(unmanaged low price ethernet switch)의 개발이 필요한 것이다. 이더넷 스위치는 여러 개의 이더넷 세그먼트 패킷을 효율적으로 다른 세그먼트에 배송할 수 있어 결과적으로 네트워크의 트래픽을 줄일 수 있다. 따라서 이더넷 스위치의 다수 포트에 각각 다수의 단말기를 연결하여 LAN의 충돌을 하지 않고 데이터 통신을 수행할 수 있으며, 다수의 단말기중 호스트 단말을 지정하여 각종 중요한 정보를 저장하게 된다. 그런데, 외부로부터 접속된 헤커(Hacker)로부터 보호하기 위해 이더넷 스위치에 워크스테이션(Workstation)을 연결하고 그 워크스테이션에 호스트 단말기를 접속하여 워크스테이션에 파이어웰(Wire Wall)을 장착하여 IP어드레스를 등록시켜 놓은 후 외부 단말기와 접속되었을 시 IP어드레스를 비교하여 IP어드레스가 일치할 경우에만 호스트 단말기와 통신이 가능하도록 패스를 연결시키고 있다. 그런데 이러한 방법은 헤커들이 IP스푸핑(Spoofing)이라는 헤킹(Hacking)기술을 사용하게 되면 일반 유닉스 서버의 보안을 위해 접근 가능한 IP어드레스를 등록하여 외부접근을 차단하여 Fire Wall이라는 보안기능을 무용지물로 만들어 호스트단말기에 저장된 중요정보들에 대하여 보안을 보장받을 수 없는 문제가 있었다.

【발명이 이루고자 하는 기술적 과제】

<6> 따라서 본 발명의 목적은 이더넷 스위치에서 MAC어드레스를 이용하여 외부의 접근을 제한하는 통신제한 방법을 제공함에 있다.

【발명의 구성 및 작용】

<7> 이하 본 발명에 따른 바람직한 실시 예를 첨부한 도면을 참조하여 상세히 설명한다. 그리고 본 발명을 설명함에 있어서, 관련된 공지 기능 혹은 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

<8> 도 1은 본 발명의 실시예에 따른 패킷 스위치 장치의 일 예를 도시한다.

<9> 호스트(100)는 패킷 스위치 장치의 전반적인 동작을 제어한다. 그리고 호스트(100)는 가장 높은 계층(Layer)을 담당하며, 패킷 스위치 장치 자체에 입력되는 명령을 수행한다. 제1 MAC 포트(110) 내지 제n MAC 포트(1n0)는 다른 패킷 스위치 장치 또는 라우터 또는 PC에 연결될 수가 있으며, 표준 MAC 제어를 수행하여 데이터 패킷 송/수신 명령을 송/수신 제어부(120)로 출력한다. 데이터 교환부(130)는 송/수신 제어부(120)의 제어에 의해, 상기 호스트(100), 제1 MAC 포트(110) 내지 제n MAC 포트(1n0)와 패킷 메모리(150)간의 데이터와 제어신호의 경로를 설정하며, 예를들어 다중화/역다중화기로 구현될 수가 있다.

<10> 서치 메모리(140)는 수신된 패킷의 목적지 어드레스에 해당하는 출력 MAC 포트를 판단하는 정보를 저장하며, 등록되어 있는 맥 어드레스를 찾을 수 있게 한다. 그리고 패킷 메모리(150)는 어드레스 테이블(152), 포트 테이블(154) 및 패킷 디스크립터(Descriptor)(156)와 같은 복수개의 정보 리소스들을 구비한다. 또한 패킷 메모리(150)는 입력되는 데이터 패킷을 저장한다. 어드레스 테이블(152)은 맥 어드레스에 대한 정보를 저장하며, 포트 테이블(154)은 각 MAC 포트들의 상태정보와 인에이블 정보, 수신 동작 완료 정보등을 저장한다. 그리고 패킷 디스크립터(156)는 패킷 메모리(150)에 저장된

각 패킷들의 정보(예:패킷 연결정보)를 저장한다.

<11> 송/수신 제어부(120)는 상기 패킷 송/수신 명령에 따라 제1 MAC 포트(110) 내지 제n MAC 포트(1n0)를 통하여 입/출력되는 패킷의 송/수신 제어를 수행한다. 즉, 송/수신 제어부(120)는 수신된 데이터 패킷을 일시 저장하며, 서치 메모리(140)를 억세스하여 수신 패킷의 헤더(Header)의 목적지 어드레스가 등록되어 있는 어드레스인지를 검사하고, 등록되어 있는 맥 어드레스 정보가 어드레스 테이블(152)의 어디에 저장되어 있는지를 알아낸다. 그리고 송/수신 제어부(120)는 상기 수신 패킷이 출력될 MAC 포트를 결정한다.

<12> 그리고 송/수신 제어부(120)는 어드레스 테이블(152), 포트 테이블(154) 및 패킷 디스크립터(156)를 억세스하여, 수신되는 데이터 패킷을 패킷 메모리(150)에 저장한다. 그리고 패킷 송신시, 송/수신 제어부(120)는 어드레스 테이블(152), 포트 테이블(154) 및 패킷 디스크립터(156)를 억세스 하여, 패킷 메모리(150)에 저장된 데이터 패킷을 해당 출력 포트를 통하여 전송한다.

<13> 도 2는 본 발명의 실시예에 따른 미디어 억세스 제어어드레스에 의해 통신을 제한하기 위한 제어흐름도이고,

<14> 도 3은 본 발명의 실시예에 따른 안티헤커 테이블 구성도이다.

<15> 상술한 도 1 내지 도 3을 참조하여 본 발명의 바람직한 실시예의 동작을 상세히 설명한다.

<16> 본 발명의 통신을 제한하기위한 ANTI HACKER를 구성하는 데이터 베이스는 두 개의 구조로 구성되어 있다. 하나는 보안(Security)를 원하는 호스트와 통신을 할 수 있는 노

드들을 관리하기 위한 _hackertbl이며 그 구조는 하기와 같이 구성된다.

<17> struct_hackertbl{

<18> u32 Hostid;

<19> u32 ipAddress

<20> u8 eTHERaDDRESS[6];

<21> u16 Port;

<22> struct_hackertbl *Next_Hostlndex;

<23> struct_hackertbl *Prev_hOSTlndex;

<24> struct_hackertbl *Next_Nodelndex[MAX_SECURITY_HOSTS];

<25> struct_hackertbl *Pre_Nodelndex[MAX_SECURITY_HOSTS];

<26> 다른 하나는 이들 포인터를 유지하기 위한 Anti-Hacker Header목적의 _hackerhead로 하기와 같이 구성된다.

<27> struct_hackerhead{

<28> u32 Hostid_List[MAX_SECURITY_HOSTS};

<29> struct_hackertbl *StartHostlndex;

<30> struct_hackertbl *EndtHostlndex;

<31> _hackertbl의 주요 멤버들을 살펴보면, 보완을 보장받기 원하는 Host의 리스트를 관리하기 위한 포인터(*Next_Hostlndex, *Prev_Hostlndex)와, 해당 호스트와 통신이 허가된 노드들의 리스트를 관리하기 위한 포인터(*, Next_Nodelndex[], *Prev_Nodelndex[]). *XXXX_Nodelndex의 인덱스로 사용하게 될 Host ID, Host의 IP와 이

더넷 어드레스, 포트넘버가 있다.

<32> _hackerhead의 주요 멤버들을 살펴보면, 보안호스트의 ID를 관장하는 Array(HostID_List), 보안을 원하는 Host List의 시작 호스트와 종료호스트를 유지하는 포인터(*StartHostIndex, *EndHostIndex)가 있다.

<33> 이와같이 구성된 2개의 데이터 구조를 기반으로 형성되는 Anti-HACKER의 데이터 베이스는 도 3과 같이 형성된다.

<34> 도 3과 같이 형성된 이더넷 스위치에서 Anti-HACKER의 데이터베이스에 해당 호스트와 통신을 허가하기 위한 노드를 등록하는 동작을 도 2의 흐름도를 참조하여 설명하면, 201단계에서 호스트(100)을 통해 보안호스트(Security Host)와 억세스 노드 어드레스를 입력한다. 보안호스트(Security Host)와 억세스 노드 어드레스를 입력명령은 ahaddhost< 00:00:f0:aa:bb:cc 168.219.83.147가 될 수 있다. 여기서 00:00:f0:aa:bb:cc는 맥어드레스이고, 168.219.83.147는 IP어드레스가 된다. 이러한 명령을 입력하면 송수신제어부(120)는 이를 수신하여 202단계에서 패킷메모리(150)의 어드레스 테이블(152)에 입력된 해당 맥 어드레스(MAC ADDRESS)가 있는가 검사하여 입력된 해당 맥 어드레스(MAC ADDRESS)가 있으면 203단계로 진행한다. 상기 203단계에서 해당 맥 어드레스의 억세스벡터(Acess Vector)를 보안키(Security Key)로 사용하기 위한 값으로 변경하여 도 3의 안티헤커(Anti-Hacker) 테이블에 포트번호를 포함하여 각각의 엔트리를 추가한다. 그리고 204단계에서 보안기능을 설정하고 205단계로 진행한다. 상기 205단계에서 어드레스 엔트리에 보안기능 설정에 따른 정보를 업데이트한다. 그러나 상기 202단계에서 어드레스 엔트리에 해당하는 맥 어드레스 없으면 206단계로 진행하여 포트번호 없이 헤커테이블에 각각의 엔트를 추가한다. 그리고 207단계에서 어드레스 엔트리 추가를 어드레스 폴트

(Fault) 프로세스에서 처리한다. 그런 후 208단계에서 어드레스 폴트를 발생하고 209단계로 진행한다. 상기 209단계에서 패킷메모리(150)의 어드레스 테이블(152)에 입력된 해당 맥 어드레스(MAC ADDRESS)가 있는가 검사하여 입력된 해당 맥 어드레스(MAC ADDRESS)가 있으면 210단계로 진행한다. 상기 210단계에서 해당 맥 어드레스의 억세스벡터(Acess Vector)를 보안키(Security Key)로 사용하기 위한 값으로 변경하여 도 3의 안티헤커(Anti-Hacker) 테이블에 포트번호를 포함하여 각각의 엔트리를 추가한다. 그리고 211단계에서 보안기능을 설정하고 212단계로 진행한다. 상기 212단계에서 어드레스 엔트리에 보안기능 설정에 따른 정보를 업데이트한다.

<35> 이와 같이 해당 호스트와 통신을 허가하는 노드들의 보안기능을 설정한 후 호스트와 통신을 수행하는 동작을 설명한다.

<36> 제1 내지 제 n MAC포트(110~1nn)을 통해 노드에서 호스트와 통신을 위해 패킷을 송신하면 송수신 제어부(120)는 이 패킷을 수신하여 어드레스 분석을 하게 되는데, 이때 이더넷 스위치는 분석과정의 일부분으로 목적지 호스트의 보안키값인 억세스 벡터값이 소스(Source)인 노드의 제한키로서 억세스 벡터에 세트되어 있는지 판단한다. 이때 억세스 벡터가 세트되어 있는 경우 정상적인 동작을 수행하지 만 세트되어 있지 않으면 해당 패킷을 버리게 된다.

【발명의 효과】

<37> 상술한 바와 같이 본 발명은 이더넷 스위치에서 호스트와 통신하기 노드들을 미리 등록시켜 놓은 후 권한이 주어지지 않은 노드들에 대한 접근을 원천적으로 로우 레이어상에

서 방지할 수 있도록 하여 헤킹을 시도하기 위한 환경을 형성하지 않도록 강력한 보안을 제공할 수 있는 이점이 있다.

【특허청구범위】

【청구항 1】

미디어 억세스 제어 어드레스에 의한 통신제한방법에 있어서,

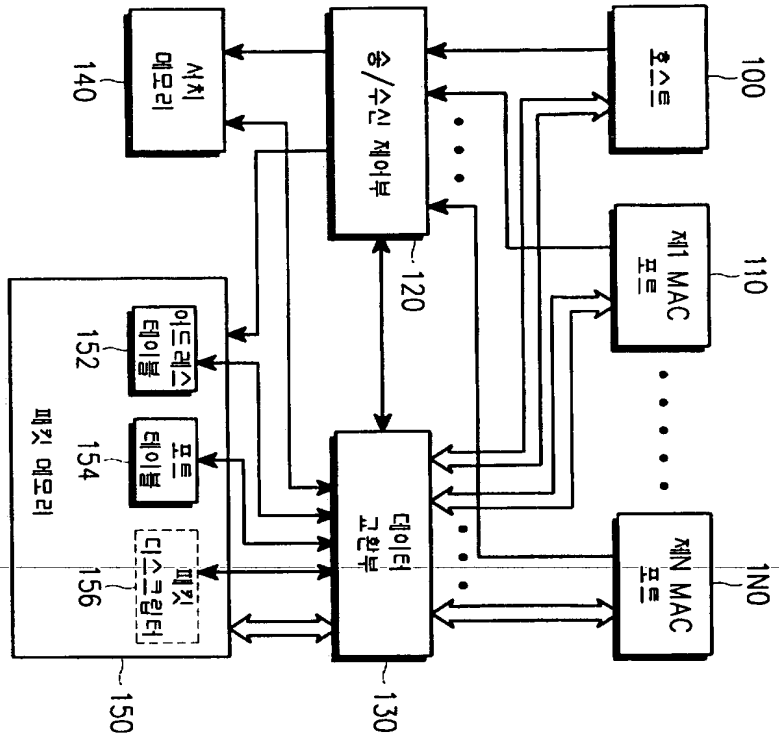
이더넷 스위치를 통해 통신요구가 있을 시 패킷데이터를 수신하는 과정과,

상기 수신한 패킷데이터의 패킷어드레스와 소스어드레스를 독출하여 각 어드레스의 엔트리 테이블 억세스 벡터가 일치하는지 검출하는 과정과,

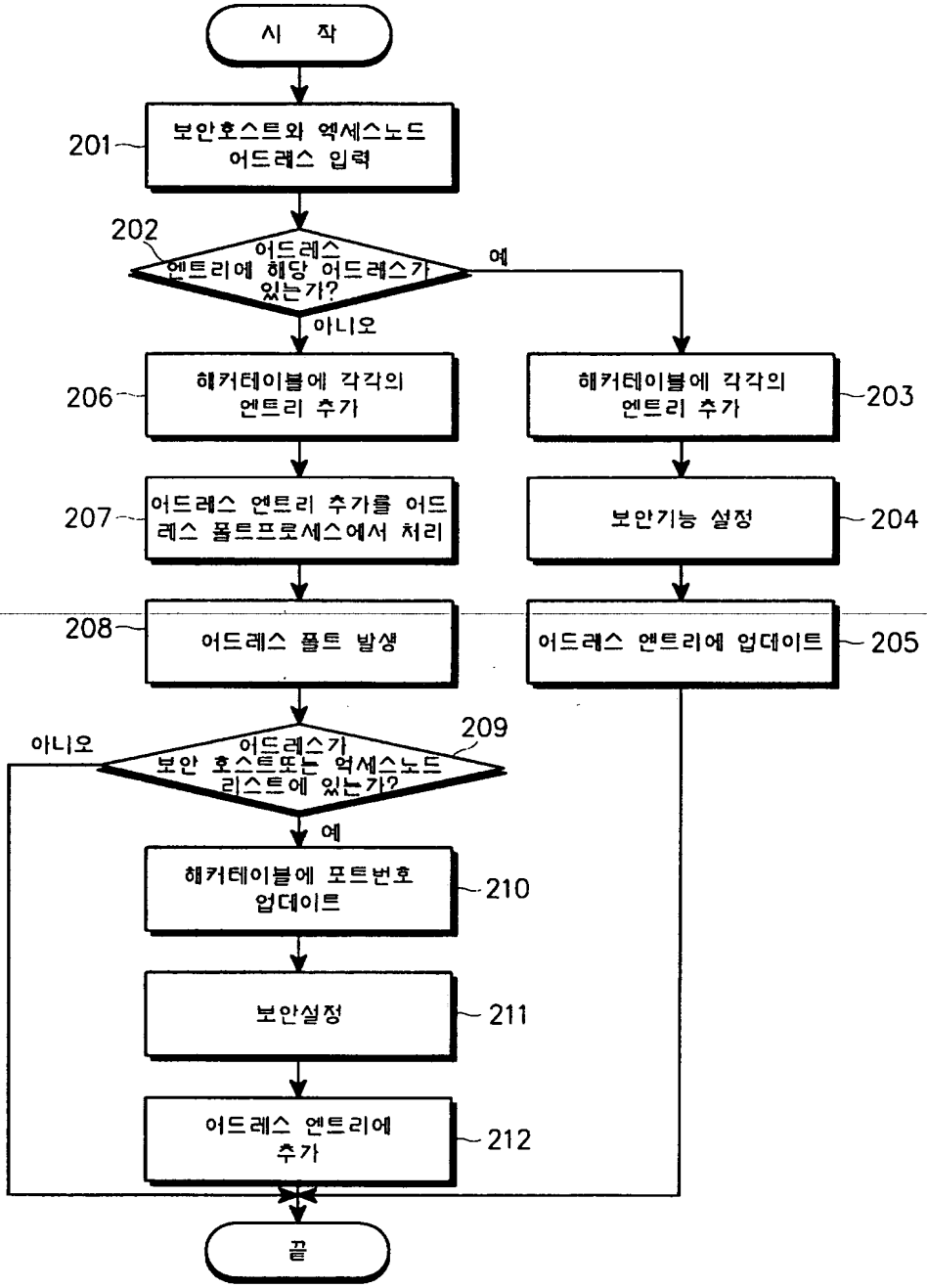
상기 엔트리 테이블 억세스벡터가 일치하지 않을 시 접속을 차단하는 과정으로 이루어짐을 특징으로 하는 미디어 억세스 제어 어드레스에 의한 통신제한방법.

【도면】

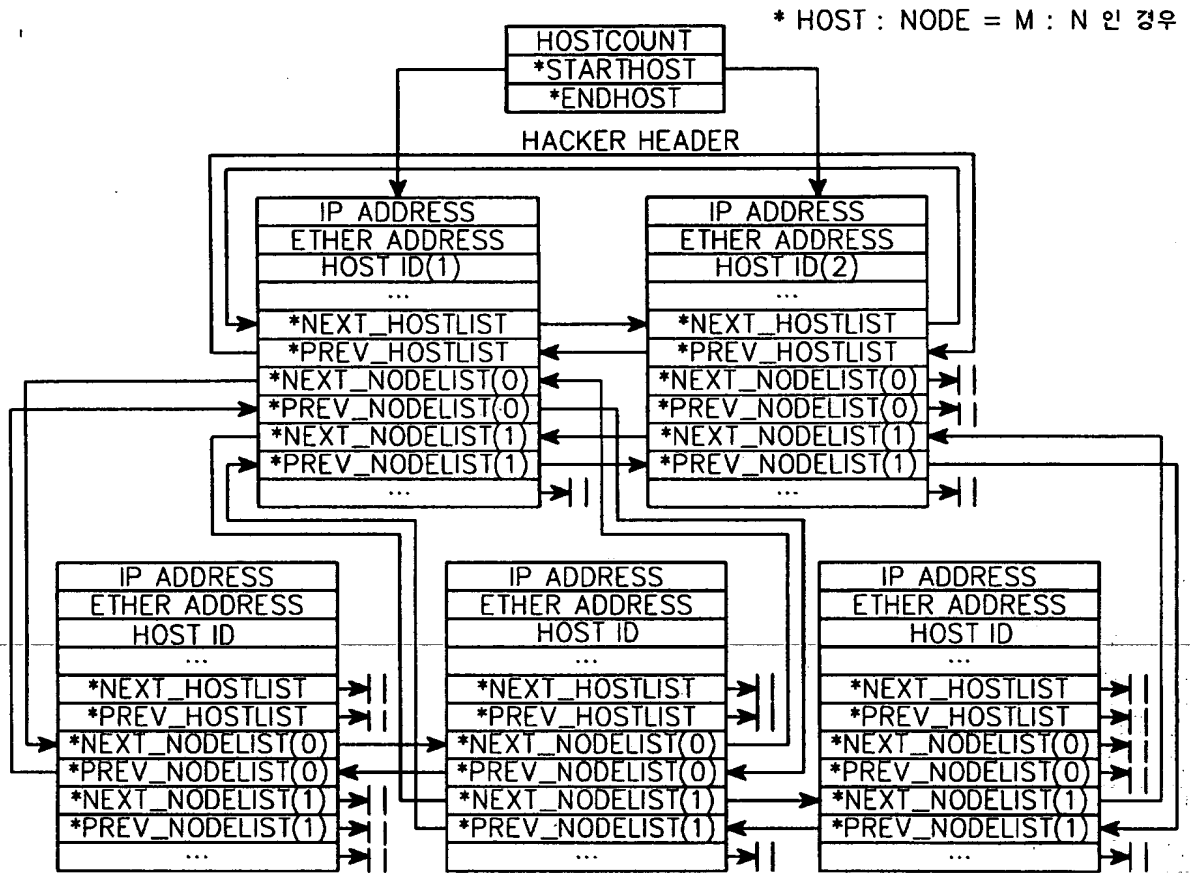
【도 1】


호스트
100
송/수신 제어부
120
상태 메모리
140
제1 MAC 포트
110
제N MAC 포트
1N0
데이터 교환부
130
패킷 메모리
150
어드레스 테이블
152
포트 테이블
154
패킷 디스크립터
156

【도 2】


시 작
보안호스트와 엑세스노드 어드레스 입력
201
202
어드레스 엔트리에 해당 어드레스가 있는가?
예
아니오
해커테이블에 각각의 엔트리 추가
206
어드레스 엔트리 추가를 어드레스 폴트프로세스에서 처리
207
어드레스 폴트 발생
208
해커테이블에 각각의 엔트리 추가
203
보안기능 설정
204
어드레스 엔트리에 업데이트
205
209
어드레스가 보안 호스트또는 억세스노드 리스트에 있는가?
아니오
예
해커테이블에 포트번호 업데이트
210
보안설정
211
어드레스 엔트리에 추가
212
끝

【도 3】


* HOST : NODE = M : N 인 경우
HOSTCOUNT
*STARTHOST
*ENDHOST
HACKER HEADER
IP ADDRESS
ETHER ADDRESS
HOST ID(1)
...
*NEXT_HOSTLIST
*PREV_HOSTLIST
*NEXT_NODELIST(0)
*PREV_NODELIST(0)
*NEXT_NODELIST(1)
*PREV_NODELIST(1)
...
IP ADDRESS
ETHER ADDRESS
HOST ID(2)
...
*NEXT_HOSTLIST
*PREV_HOSTLIST
*NEXT_NODELIST(0)
*PREV_NODELIST(0)
*NEXT_NODELIST(1)
*PREV_NODELIST(1)
...
IP ADDRESS
ETHER ADDRESS
HOST ID
...
*NEXT_HOSTLIST
*PREV_HOSTLIST
*NEXT_NODELIST(0)
*PREV_NODELIST(0)
*NEXT_NODELIST(1)
*PREV_NODELIST(1)
...
IP ADDRESS
ETHER ADDRESS
HOST ID
...
*NEXT_HOSTLIST
*PREV_HOSTLIST
*NEXT_NODELIST(0)
*PREV_NODELIST(0)
*NEXT_NODELIST(1)
*PREV_NODELIST(1)
...
IP ADDRESS
ETHER ADDRESS
HOST ID
...
*NEXT_HOSTLIST
*PREV_HOSTLIST
*NEXT_NODELIST(0)
*PREV_NODELIST(0)
*NEXT_NODELIST(1)
*PREV_NODELIST(1)
...